IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the Application:

LISTING OF CLAIMS:

1. (Currently Amended) A computer-implemented method for creating an order- invariant fuzzy commitment, comprising:
(a) receiving a first input element comprising a sequence of at least one value ($a_1,\ldots, a_n$) from a predetermined set;
(b) generating a codeword of an error-correcting code for generating the commitment;
(c) constructing a first sequence of coordinate sets ($x_i,y_i$), for i in {1,...n}, each of the coordinate sets having a first value ($x_i$) corresponding to a representation of an associated one ($a_i$) of the at least one value of the first input element and a second value ($y_i$) corresponding to a symbol in the codeword, wherein the symbol corresponds to the $x_i$th symbol in the codeword, wherein an order-invariant fuzzy commitment is formed, the commitment having the property that it may be algorithmically combined with at least one set of values comprising at least one value of the first input element so as to yield the codeword;

reordering the first sequence based upon the first value; ~~and~~

outputting the first sequence; and

utilizing the first sequence, in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence.

2. (Previously Presented) The method according to claim 1, wherein the representation of the first value in the first sequence of coordinate sets is an integer representation.

3. (Cancelled)

4. (Original) The method according to claim 1, further including deriving the first input element from a measurement of a biometric associated with a user.

5. (Original) The method according to claim 4, further including selecting the biometric from the group consisting of fingerprint information, retinal scan information, iris scan information, bloodflow-pattern information, thermal imaging information, handwritten-signature dynamics information, physiognomic information, hand geometry information, and voice information.

6. (Original) The method according to claim 1, further including adding chaff to the first sequence.

7. (Original) The method according to claim 6, further including adding the chaff as sets of pairs of the form (x,y) such that x does not lie in the input sequence and y is generated at random.

8. (Original) The method according to claim 6, further including adding the chaff as sets of pairs of the form (x,y) such that one or more values x do lie in the input sequence and y is generated at random.

9. (Currently Amended) A computer-implemented method for creating an order-invariant fuzzy commitment, comprising:
(a) receiving a first input element comprising a sequence of at least one value $(a_1,\ldots,a_n)$ from a predetermined set;
(b) generating a codeword of an error-correcting code for generating the commitment;

(c) constructing a first sequence of coordinate sets $(x_i,y_i)$,for i in {l,...n}, each of the coordinate sets having a first value $(x_i)$ corresponding to a representation of an associated one $(a_i)$ of the at least one value of the first input element and a second value $(y_i)$ corresponding to a symbol in the codeword, wherein the symbol corresponds to the $x_i$th symbol in the codeword, wherein an order-invariant fuzzy commitment is formed, the commitment having the property that it may be algorithmically combined with at least one set of values comprising at least one value of the first input element so as to yield the codeword;

adding the chaff as sets of pairs of the form (x,y) such that x does not lie in the input sequence and y is generated at random; and

reordering the first sequence based upon the first value; ~~and~~

outputting the first sequence; and

utilizing the first sequence, in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence.

10. (Original) The method according to claim 9, further including reordering the first sequence in ascending order based upon the first value.

11. (Original) The method according to claim 1, further including applying a bijective function to an input secret to obtain the codeword for the symbol corresponding to the second value.

12. (Original) The method according to claim 1, further including decommitting the order-invariant commitment by

receiving a second input element including a second sequence of at least one value $(b_1,\ldots, b_m)$ from the predetermined set;

receiving the first sequence;

constructing a derived set of values $(X' = x_1', \ldots, x_m')$ representing respectively the at least one value $(b_1, \ldots, b_m)$ in the second sequence;

selecting a subset of the coordinate sets $\{(x_i, y_i)\}$ in the first sequence (E) such that for each pair (x',y') in the subset, the first value in the pair (x') lies in the derived set of values (X'); and

applying an error-correcting function to the subset.

13. (Original) The method according to claim 12, wherein the error-correcting function includes a Reed-Solomon code.

14. (Original) The method according to claim 1, further including selecting a polynomial to generate the codeword.

15. (Original) The method according to claim 1, further including utilizing a decodable design for decommiting the order-invariant commitment.

Claims 16-17 (Cancelled).

18. (Currently Amended) A computer-implemented method for creating a reordering-tolerant fuzzy commitment comprising:

(a) receiving a first input element A including a first sequence of at least one value;

(b) generating a first codeword c of an error-correcting code for the commitment;

(c) constructing a sequence E of one or more data elements responsive to the first input element A and the first code word c of the error-correcting code [[c]];

(d) outputting the sequence E;

(e) receiving a second input element B including a second sequence of at least one value and the sequence E, wherein the second sequence has a number of elements m;

(f) applying a function d responsive to the second input element B and the sequence E, wherein the function yields as output a value of a second codeword (c' d(B,E)), the function having a property such that d(V,E) =c for at least one possible value of V, where V comprises a third sequence having a number of elements $m_v$, wherein the at least one value of the first sequence differs from the at least one value of the third sequence in at least $m_v$ /2 values; ~~and~~

(g) outputting the second codeword [[c']] (c' d(B,E)); and

(h) utilizing the second codeword (c' d(B,E), in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence.

19. (Currently Amended) A computer-implemented method for generating an order invariant fuzzy commitment of an item of information, comprising:

receiving a first set of elements;

selecting a polynomial for encoding the item under the first set of elements to generate an order-invariant fuzzy commitment of the item; ~~and~~

generating the order-invariant fuzzy commitment of the item;

storing said commitment in a computing device; and

utilizing the commitment, in response to receiving a second set of elements from a user, to authenticate the user to a secured system associated with the commitment.

20. (Original) The method according to claim 19, further including inserting chaff points that form a part of the commitment of the item.

21. (Original) The method according to claim 19, further including

receiving a second set of elements; and

selectively decommitting the item based upon a level of overlap of the first and second sets of elements.

22. (Original) The method according to claim 21, further including determining the polynomial from the second set of elements if the level of overlap is greater than a predetermined threshold.

23. (Original) The method according to claim 21, further including utilizing an error-correcting code for determining the polynomial.

24. (Currently Amended) The method according to claim 23, further including utilizing a Reed-Solomon error detecting code to add redundancy symbols configured to correct errors in the first set of elements.

25. (Original) The method according to claim 19, wherein the first set of elements corresponds to a biometric template.

26. (Original) The method according to claim 19, further including utilizing a decodable design to decommit the item, wherein the decodable design includes constituent pairs of sets having a level of overlap less than a predetermined level.

27. (Original) The method according to claim 19, further including hiding the first set of elements in a target set containing a plurality of elements selected from a field.

28. (Original) The method according to claim 27, further including projecting the first set of elements onto the target set.

29-37. (Cancelled)

38. (Currently Amended) An article comprising a tangible machine readable medium that stores executable code instructions enabling a machine to perform the steps of:

(a) receiving a first input element comprising a sequence of at least one value from a predetermined set;

(b) generating a codeword of an error-correcting code; and

(c) constructing a first sequence of coordinate sets, each of the coordinate sets having a first value corresponding to a representation of an associated one of the at least one value of the first input element and a second value corresponding to a symbol in the codeword, wherein the symbol is associated with the corresponding first value;

further including code for enabling the steps of

receiving a second input element including a second sequence of at least one value from the predetermined set;

receiving the order-invariant fuzzy commitment;

constructing a set of values representing respectively the values in the second sequence;

selecting a subset of the coordinate sets in the first sequence such that the first value in each subset coordinate set corresponds to the first value of at least one coordinate set in the first sequence; ~~and~~

applying an error-correcting function to the subset; and

authenticating a user associated with the second input element to a secured system associated with the first sequence.

Claim 39 (Cancelled).

40. (Currently Amended) A computer-implemented method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one value ($a_1$,..., $a_n$) from a predetermined set (F);

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (E) of coordinate sets $(x_i,y_i)$, for i in {1,...k} for integer k > 0, each of the coordinate sets having a first value $(x_i)$ corresponding to a representation of an associated one $(a_j)$ of the at least one value of the first input element (A) and a second value $(y_i)$ corresponding to a symbol in the codeword (c), wherein the symbol is selected in a manner responsive to the first value $x_i$, wherein an order-invariant fuzzy commitment is formed;

reordering the first sequence based upon the first value; ~~and~~

outputting the first sequence; and

utilizing the first sequence, in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence.

41. (Currently Amended) A computer-implemented method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one value $(a_1,..., a_n)$ from a predetermined set (F);

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (E) of coordinate sets $(x_i,z_i,y_i)$, for i in {1,...,k} for integer k > 0, each of the coordinate sets having a first value $(x_i)$ corresponding to a representation of an associated one $(a_i)$ of the at least one value of the first input element (A) and a second value $(z_i)$ constructed in a manner responsive to a pattern of occurrence of the associated one $(a_i)$ of the at least one value of the first input element (A) in the sequence $(a_1,..., a_n)$ and a third value $(y_i)$ corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the

first and second values of the coordinate set ($x_i$ and $z_i$), wherein an order-invariant fuzzy commitment is formed; ~~and~~

(d) outputting the first sequence; and

(e) utilizing the first sequence, in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence.

42. (Original) The method according to claim 41, further including decommitting the order-invariant commitment by

receiving a second input element (B) including a second sequence of at least one value ($b_1$, ..., $b_m$) from the predetermined set (F);

receiving the first sequence (E);

constructing a derived set of values (X' = x1', ... , $x_m$') representing respectively the at least one value ($b_1$, ..., $b_m$) in the second sequence (B);

selecting a subset (E') of the coordinate sets {($x_i$, $y_i$)} in the first sequence (E) such that for each pair (x',z',y') in the subset (E'), the first value in the pair (x') lies in the derived set of values (X'); and

applying an error-correcting function to the subset (E').

43. (Currently Amended) A computer-implemented method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one value ($a_1$,. . ., $a_n$) from a predetermined set;

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (E) of coordinate sets ($x_i$,$z_i$,$y_i$), for i in {1 ,...,k} for integer k > 0, each of the coordinate sets having a first value ($x_i$) corresponding to a representation of an associated one ($a_i$) of the at least one value of the first input element (A) and a second value ($z_i$) constructed in a manner responsive to information in the first input element (A), and a third value

($y_i$) corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values ($x_i$ and $z_i$) of the coordinate set, wherein an order-invariant fuzzy commitment is formed; ~~and~~

(d) outputting the first sequence; and

(e) utilizing the first sequence, in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence.

44. (Original) The method according to claim 43, further including decommitting the order-invariant commitment by

receiving a second input element (B) including a second sequence of at least one value ($b_1$, ..., $b_m$) from the predetermined set (F);

receiving the first sequence (E);

constructing a derived set of values (X' $x_1$', , $x_m$') representing respectively the at least one value ($b_1$, ..., $b_m$) in the second sequence (B); and

selecting a subset (E') ofthe coordinate sets {( $x_i$,$y_i$)} in the first sequence (E) such that for each pair (x',z',y') in the subset (E'), the first value in the pair (x') lies in the derived set of values (X'); and

applying an error-correcting function to the subset (E').

45. (Currently Amended) A computer-implemented method for creating an order-invariant fuzzy commitment, comprising:

(a) receiving a first input element (A) comprising a sequence of at least one pair of values ($a_1$,$w_1$), ($a_2$,$w_2$),,..., ($a_n$,$w_n$) wherein each of the at least one $a_i$ values is from a first predetermined set (F) and each of the at least one $w_i$ values is from a second predetermined set (G);

(b) generating a codeword (c) of an error-correcting code for generating the commitment;

(c) constructing a first sequence (B) of coordinate sets $(x_i,z_i,y_i)$, for i in {l,...,k} for integer k > 0, each of the coordinate sets having a first value $(x_i)$ corresponding to a representation of an associated one $((a_i,w_i))$ of the at least one pair of values of the first input element (A) and a second value $(z_i)$ constructed in a manner responsive to an associated one $((a_i,w_i))$ of the at least one value of the first input element (A) in the sequence $(a_1,w_1)$, $(a_2,w_2)$,,..., $(a_n,w_n)$ and a third value $(y_i)$ corresponding to a subset of symbols in the codeword (c), wherein the subset of symbols is selected in a manner responsive to at least one of the first and second values of the coordinate set ($x_i$ and $z_i$), wherein an order-invariant fuzzy commitment is formed; ~~and~~

outputting the first sequence; and

utilizing the first sequence, in response to receiving a second input element from a user, to authenticate the user to a secured system associated with the first sequence.

46. (New) The method of claim 4, further including decommitting the order-invariant commitment by:

receiving a second input element including a second sequence of at least one value $(b_1,..., b_m)$ from the predetermined set, the second input element being derived from a measurement of a biometric associated with a user;

receiving the first sequence;

constructing a derived set of values $(X' = x_1', ... , x_m')$ representing respectively the at least one value $(b_1, ..., b_m)$ in the second sequence;

selecting a subset of the coordinate sets $\{(x_i, y_i)\}$ in the first sequence (E) such that for each pair (x',y') in the subset, the first value in the pair (x') lies in the derived set of values (X');

applying an error-correcting function to the subset; and

authenticating the user to the secured system associated with the first sequence.